

地方税共同機構
情報セキュリティポリシー
【基本方針】
4.0版

地方税共同機構
平成31年4月1日地税機規程第23号

<変更履歴>

| 項番 | 変更日 | 版数 | 変更内容 | 変更箇所 |
|----|----------|-----|-------------------------------|---------------------------------------|
| 1 | 2019/4/1 | 4.0 | 地方共同法人化に伴う名称、組織及び情報資産対象範囲の変更等 | e L T A X情報セキュリティポリシー基本方針 3.1版を基に全面改訂 |
| | | | | |

< e L T A X情報セキュリティポリシー基本方針変更履歴 >

| 項番 | 変更日 | 版数 | 変更内容 | 変更箇所 |
|----|-----------|-----|-------------------------------|-------------|
| 1 | 2012/4/1 | 2.3 | 軽微な修正 | 2.2版を基に改訂 |
| 2 | 2013/5/15 | 3.0 | 「登録委託先事業者」という表現を「認定委託先事業者」に変更 | 2.3版を基に全面改訂 |
| 3 | 2014/2/13 | 3.1 | 協議会の体制変更の反映及び整理 | 3.0版を基に改訂 |

目次

| | |
|--------------------------|---|
| 第1章 目的 | 1 |
| 第2章 ポリシーが遵守すべき法令等 | 1 |
| 第3章 ポリシーの構成 | 2 |
| 第4章 基本方針の内容 | 2 |
| 第5章 対策基準の内容 | 2 |
| 第6章 定義 | 2 |
| 第7章 適用範囲 | 5 |
| 第8章 役職員等の遵守義務 | 6 |
| 第9章 対象とする脅威 | 6 |
| 第10章 情報セキュリティ対策 | 6 |
| 第11章 地方団体の役割 | 7 |
| 第12章 ポリシーの公開等 | 7 |
| 第13章 実施手順の策定 | 8 |
| 第14章 情報セキュリティ監査及び自己点検の実施 | 8 |
| 第15章 ポリシーの見直し | 8 |
| 第16章 留意事項（用語の読み替えについて） | 8 |

第1章 目的

地方税共同機構（以下「機構」という。）は、納税義務者等に係る地方税の極めて重要な情報を取り扱うことから、高い安全性と信頼性が確保できる運営を求められている。

このことから、情報資産を適切に取り扱うための基本的な方針及び遵守すべき事項や判断の基準として地方税共同機構情報セキュリティポリシー（以下「ポリシー」という。）を策定する。

また、機構の役員、職員、非常勤職員、臨時職員及び派遣職員（以下「役職員等」という。）並びに委託先事業者及び認定委託先事業者は、ポリシーを遵守し、次の諸点を常に念頭に置いて情報資産の取り扱うことが責務として課せられている。

- 機構のすべての役職員等、委託先事業者及び認定委託先事業者は、情報セキュリティ対策が重大かつ喫緊の課題であることを常に認識し、矜持を持って様々な脅威に対応すること
- 情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続すること
- 情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくこと
- 情報セキュリティに関する事故の未然防止のみならず、事故が発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくこと

第2章 ポリシーが遵守すべき法令等

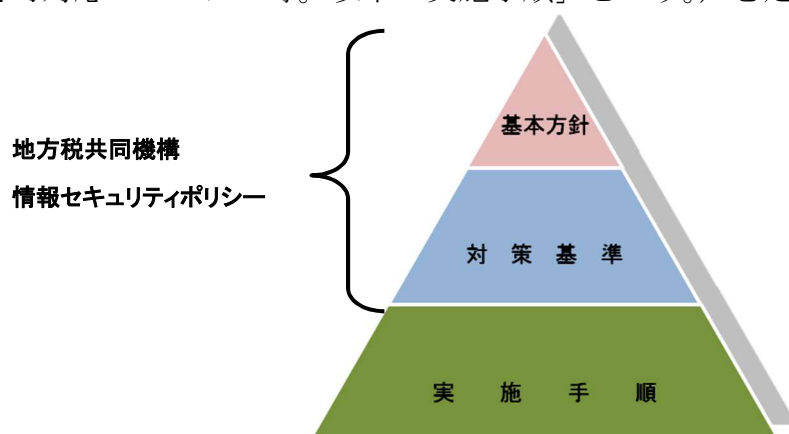
機構のすべての役職員等、委託先事業者及び認定委託先事業者は、上記の目的を達成するため、地方税法等の関連する法令等を遵守する。特に、「地方税法施行規則第24条の40第3項第2号及び第3号に規定する電気通信回線その他の電気通信設備に関する技術基準及び情報通信の技術の利用における安全性及び信頼性を確保するために必要な事項に関する基準（平成31年総務省告示第151号）（以下「国税連携技術基準」という。）」、「地方税法施行規則第10条第5項及び第24条の39第3項に規定する情報通信の技術の利用における安全性及び信頼性を確保するために必要な基準（平成31年総務省告示第146号）（以下「電子申告等安全性基準」という。）」、「地方税法施行規則第24条の42第3項に規定する特定徴収金及び特定徴収金に関する情報の取扱いにおける安全性及び信頼性を確保するために必要な基準（平成31年総務省告示第149号）（以下「共通納税安全性基準」という。）」、「地方税法施行規則第9条の8第4項に規定する情報通信の技術の利用における安全性及び信頼性を確保するために必要な事項に関する基準（平成31年総務省告示第153号）（以下「年金安全性基準」という。）」、「地方税法施行規則第9条の3の2第1項に規定する情報通信の技術の利用における安全性及び信頼性を確保するために必要な事項に関する基準（平成31年総務省告示第152号）（以下「特別徴収税額通知安全性基準」という。）」、「行政手続における特定の個人を識別するための番号の利用等に関する法律施行規則第20条第3号の規定に基づき内閣総理大臣が定める基準（平成27年内閣府告示第447号）（以下「内閣府技術基準」という。）」に適合するポリシーを制定し、セキュリティ対策を実施する。

また、「地方公共団体における情報セキュリティポリシーに関するガイドライン」等を適宜参考するものとする。

第3章 ポリシーの構成

ポリシーは、一定の普遍性をもった部分（情報セキュリティポリシー基本方針。以下「基本方針」という。）と、技術水準等情報セキュリティに関する社会状況の変化を的確に反映させ、基本方針の具体化を図る部分（情報セキュリティポリシー対策基準。以下「対策基準」という。）の2部をもって構成するものとする。

また、対策基準について、具体的に情報システムに展開する場合の、個別の実施事項を定めるものとして、情報セキュリティポリシーに係る実施手順（アクセス実施管理手順や緊急時対応マニュアル等。以下「実施手順」という。）を定める。



第4章 基本方針の内容

基本方針は、ポリシーの目的、適用範囲、情報セキュリティに対する取り組み姿勢など基本的な考えを示すものであり、機構における情報セキュリティに関する最上位の規程と位置付ける。

第5章 対策基準の内容

対策基準は、基本方針を実現するため、情報セキュリティの推進体制、情報システムの開発及び運用など、情報セキュリティを確保するために遵守すべき事項又は判断の基準を示すものである。

第6章 定義

ポリシー・実施手順において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）

- (2) **情報システム**
コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組み
- (3) **e L T A X**
地方税ポータルシステムの呼称で、地方税における手続きを電子的に行うシステム
- (4) **O S S システム**
O S S 都道府県税共同利用化システムの呼称で、新車新規登録に伴う自動車二税の申告・納付手続きを電子的に行うシステム
- (5) **J N K S**
自動車税納付確認システムの呼称で、自動車税納付の確認を電子的に行うシステム
- (6) **機構処理税務事務システム**
機構が運営する税務事務に係る情報システムで、e L T A X システム、O S S システム、J N K S の総称
- (7) **e L T A X ホームページ・ヘルプデスクシステム**
e L T A X に係るホームページ・ヘルプデスクシステム及びナレッジシステム
- (8) **全国税協ホームページシステム**
全国税務地方協議会から承継したホームページシステム
- (9) **機構ホームページシステム**
e L T A X ホームページ・ヘルプデスクシステム及び全国税協ホームページシステムの総称
- (10) **地方税ポータルシステム情報サーバ**
地方税ポータルシステムを構成するサーバ
- (11) **O S S システム情報サーバ**
O S S システムを構成するサーバ
- (12) **J N K S 情報サーバ**
J N K S を構成するサーバ
- (13) **認定委託先事業者情報システム**
認定委託先事業者が開発又は運用を行っている情報システムのうち、機構処理税務事務に係る情報システム
- (14) **認定委託先事業者サーバ**
認定委託先事業者情報システムを構成するサーバ
- (15) **団体情報システム**
地方団体が開発又は運用を行っている情報システムのうち、機構処理税務事務に係る情報システム
- (16) **団体サーバ**
団体情報システムを構成するサーバ
- (17) **事務局情報システム**
機構の役職員等が使用する機構事務局の情報システム
- (18) **重要機能室**
電子計算機室、受電設備、定電圧・定周波電源装置等の設備を設置する室並びに電子

計算機室の空気調和をする空気調和機及びその付属設備を設置する室

(19) **情報セキュリティ**

情報資産の機密性、完全性及び可用性を維持すること

(20) **機密性**

情報へのアクセスを認められた者だけが、アクセス可能な状態を確保すること

(21) **完全性**

情報が破壊、改ざん又は消去されていない状態を確保すること

(22) **可用性**

情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること

(23) **利用者**

機構処理税務事務システムを利用する納税義務者（特別徴収義務者を含む。）及び代理人（税理士等）

(24) **委託先事業者**

機構から機構処理税務事務システムの開発及び運用に関する業務の委託を受けた事業者

(25) **認定委託先事業者**

認定委託先事業者の認定等に関する要綱に基づき認定された事業者

(26) **地方団体**

地方団体は、単独設置型地方団体と委託利用型地方団体に分類される。

ア 単独設置型地方団体

団体サーバに供えられたファイルへの関係書類に記載すべき事項の記録（以下「記録事務」という。）を単独で行う地方団体、並びに委託利用型団体から記録事務又は団体サーバの設置及び運営等（以下「設置運営事務」という。）を受託する団体

イ 委託利用型地方団体

記録事務（設置運営含む。）を認定委託先事業者又は単独設置型地方団体に委託する地方団体

(27) **関係者**

機構が別途定める者

(28) **情報資産**

機構に係る全ての情報システムの開発又は運用に係る全ての情報、機構に係る全ての情報システムで取り扱う全ての情報及びこれらの情報を管理するコンピュータやネットワークなどの設備

(29) **個人情報**

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述、又は個人別に付けられた番号、記号その他の符号、画像若しくは音声によって当該個人を識別できるもの（当該情報だけでは識別できないが、他の情報と容易に照合することができ、それによって当該個人を識別できる者を含む。）

(30) **破壊・改ざん**

ハードウェアやネットワークそのものの破壊だけでなく、情報の一部を不正に変更したり消去することで、業務が遂行不可能な状態になること、または、著しく遂行が妨げられること

第7章 適用範囲

(1) 組織の範囲

ポリシーが適用される組織は、機構、委託先事業者及び認定委託先事業者とする。

ア 機構及び委託先事業者に対するポリシーの適用

機構に係る全ての情報システムの開発・運用に関する業務は、機構及び地方団体の人的業務量の低減を図り、かつ、共同化のメリットである費用の低廉化を図る必要性から、原則として外部委託を行う。

このため、ポリシーの策定に当たっては、上記事情を考慮した対策基準の策定を行い、機構及び委託先事業者はポリシーの重要性を認識し、業務の遂行に当たってはポリシーを遵守する義務を負うものとする。

イ 認定委託先事業者に対するポリシーの適用

認定委託先事業者情報システムの開発・運用に関する業務は、機構及び地方団体の人的業務量の低減を図り、かつ、共同化のメリットである費用の低廉化を図る必要性から、認定委託先事業者が行う。

認定委託先事業者は、業務の遂行に当たり、ポリシーを遵守する義務を負うものとする。

ウ 地方団体に対するポリシーの適用

地方団体が導入する団体情報システムは、地方団体の管理責任のもとで構築・運用される。このため、団体情報システム並びに団体情報システムに係る情報資産、組織、人及び業務は、原則としてポリシーの適用対象外とし、団体情報システムに係る情報セキュリティ対策は、各地方団体が計画・実施すべきものとする。

ただし、機構処理税務事務システム全体の情報セキュリティを確保する観点から、団体情報システムからポータルセンターへのアクセス等の特定の業務については、一定の対策基準を策定することとする。

エ 利用者に対するポリシーの適用

機構処理税務事務システムの利用者は、ポリシーの適用外とするが、システムの利用については別に定める利用規約等の承諾を求める。

(2) 情報資産の範囲

ポリシーが対象とする情報資産は、次のとおりとする。

ア ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体。

イ ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）。

ウ すべての情報システムの仕様書及びネットワーク図等のシステム関連文書。

| | |
|--------|-------------------------------|
| ネットワーク | 通信回線、ルータ等の通信機器 |
| 情報システム | サーバ、パソコン、オペレーティングシステム、ソフトウェア等 |

| | |
|-------------------------|---|
| ネットワーク及び情報システムに関する施設・設備 | コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル |
| 電磁的記録媒体 | CD-R、DVD-R、フロッピーディスク、MO、LT0(Linear Tape-Open)、USB フラッシュメモリ等 |
| ネットワーク及び情報システムで取り扱う情報 | ネットワーク、情報システムで取り扱うデータ（利用者情報、申告情報、アクセス記録、認証情報等） ※これらを印刷した文書を含む。 |
| システム関連文書 | システム設計書、プログラム仕様書、オペレーションマニュアル、端末機管理マニュアル、システム構成図、ネットワーク構成図等 |

第8章 役職員等の遵守義務

役職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たってポリシー・実施手順を遵守しなければならない。

第9章 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

- (1) サイバー攻撃をはじめとする部外者の情報システムへの侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の搾取、内部不正等
- (2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的的要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害によるサービス及び業務の停止等
- (4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
- (5) 電力供給の途絶、通信の途絶、水道供給の途絶等の提供サービスの障害からの波及等

第10章 情報セキュリティ対策

第9章の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制

組織として、情報セキュリティ対策を確実に実施するには、情報セキュリティ対策に取り組む十分な組織体制を整備し、一元的に情報セキュリティ対策を実施する必要がある。このことから、情報セキュリティ対策のための組織体制、権限及び責任を規定する。

(2) 情報資産の分類と管理

情報資産を保護するには、情報資産を分類し、分類に応じた管理方法を定める必要がある。そこで、機密性・完全性・可用性に基づく情報資産の分類と分類に応じた取扱いを定めた上で、情報資産の管理責任を明確にし、情報資産のライフサイクルに応じた対策

を講じる。

(3) 物理的セキュリティ

ハードウェア、ネットワーク、重要機能室等は、情報システムの安定的な運用のために適切に管理する必要があり、管理が不十分な場合、情報システム全体への悪影響や業務の継続性に支障が生じるおそれがある。このことから、ハードウェアの設置や保守・管理、ネットワークの通信回線装置の管理、重要機能室の入退室管理等の物理的な対策を講じる。また、役職員等が利用するパソコン等についても盗難及び情報漏えい防止策、パソコン等の持ち出し・持ち込み等に関する対策を講じる。

(4) 人的セキュリティ

役職員等が情報資産を不正に利用したり、適正な取扱いを怠ったりした場合、コンピュータウイルス等の感染、情報漏えい等の被害が発生しうる。このことから、ポリシーの遵守や情報資産の業務以外の目的での使用の禁止等、役職員等が情報資産を取り扱う際に遵守すべき事項を明確に規定する。また、人的セキュリティを確保するための教育・研修・訓練に関する計画や実施等の人的な対策を講じる。

(5) 技術的セキュリティ

システム開発、導入、保守、運用等において、コンピュータウイルス等への不正プログラム対策や情報システムに対する攻撃への対策等、技術的なセキュリティ対策が十分に行われない場合は、業務に重大な支障が生じるおそれがある。このことから、情報システムが備えるべき技術的セキュリティの対策を講じる。

(6) ポリシーの運用

ポリシーの遵守を確保するために、ポリシーの遵守状況等を確認する体制を整備するとともに、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講じる。

第 1 1 章 地方団体の役割

機構は、地方税に関する事務の合理化並びに利用者の利便の向上に寄与することを目的に、全国の地方団体が共同して運営する組織として、機構処理税務事務を行うとともに、地方団体に対してその地方税に関する事務に関する支援を行うことを基本方針としている。よって、機構処理税務事務システムの情報セキュリティの確保には地方団体の協力が不可欠であり、地方団体は機構処理税務事務システムの運用にあたり情報セキュリティの維持向上に努めるものとする。

第 1 2 章 ポリシーの公開等

機構は、機構処理税務事務システムに対する信頼と理解を深めるため、地方団体及び利用者に対しポリシーの公開又は内容の周知を行う。また、適正なシステム開発・運用を行うため、委託先事業者に対しても同様とする。

なお、公開又は周知する対象、範囲及び内容等については、理事長が別途定める。

第13章 実施手順の策定

対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた実施手順を策定するものとする。

なお、実施手順は、公にすることにより機構の業務運営に重大な支障を及ぼすおそれがあることから地方団体及び利用者に対して非公開とし、機構の代表者会議、運営審議会、機構処理税務情報保護委員会、実務者会議又は各検討部会での公開に限るものとする。

第14章 情報セキュリティ監査及び自己点検の実施

ポリシーが遵守されていることを検証するために、機構は定期的又は必要に応じて定款第34条に定める第三者による監査として、情報セキュリティ監査を実施するとともに自己点検を実施するものとする。

第15章 ポリシーの見直し

- (1) 理事長は、ポリシーについて情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ毎年度見直しを行い、必要があると認めた場合、改善を行うものとする。
- (2) ポリシーの改廃を行った場合、地方団体等の関係者に速やかに周知しなければならない。

第16章 留意事項（用語の読み替えについて）

対策基準は機構を主体として定めているため、委託先事業者及び認定委託先事業者は特に断り書きがない場合、主体を自身に読み替えて遵守するものとする。認定委託先事業者は、機構処理税務事務システムを認定委託先事業者情報システムに読み替えて遵守するものとする。